FortiManager - Upgrade Guide

VERSION 5.6.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

July 27, 2017

FortiManager - Upgrade Guide

02-560-404512-20170727

Change Log

Date	Change Description
2017-07-27	Initial Release of 5.6.0.

FortiManager Firmware

This document provides an overview of FortiManager firmware and highlights general information you should be aware of prior to upgrading your device. This guide is intended to supplement the *FortiManager Release Notes* documentation.

The following topics are included in this section:

Best practices

Before any firmware upgrade complete the following:

- Upgrade the version of ADOMs from 5.0 to 5.2 because FortiManager supports only the following ADOM versions: 5.2, 5.4, and 5.6.
- Download the firmware image and Release Notes document from the Fortinet Customer Service & Support portal. Review the Release Notes including special notices, upgrade information, product integration and support, resolved and known issues.
- Prepare your device for upgrade. Install any pending configurations, ensure your managed devices are running the appropriate firmware versions as documented in the firmware Release Notes.
- Back up your configuration file. It is recommended that you create a system backup file and save this configuration to your local computer. The device configuration file is saved with a `.dat` extension.

In VM environments, it is recommended that you clone the VM instance. In the event of an issue with the firmware upgrade, you can revert to the VM clone.

In VM environments, upgrade your VM server to latest stable update and patch release offered by the VM host server provider.

- Plan a maintenance window to complete the firmware upgrade. If possible, you may want to set up a test environment to ensure that the upgrade does not negatively impact your network or managed devices.
- Once the upgrade is complete, test your device to ensure that the upgrade was successful and that all managed devices are listed.

Firmware best practice: Stay current on patch releases for your current major release. Only upgrade to a new major release or version when you are looking for specific functionality in the new major release or version. For more information, see the *FortiManager Release Notes* or contact Fortinet Technical Support.

Upgrading the device firmware can trigger an SQL database rebuild. During this time, new logs will not be available until the rebuild is complete. The time required to rebuild the database is dependent on the size of the database. You can use the `diagnose sql status rebuild-db` command to display the SQL log database rebuild status.

The following features will not be available until after the SQL database rebuild has completed: FortiView, Log View, Event Management, and Reports.

Firmware image naming convention

Firmware images on the Fortinet Customer Service & Support portal HTTPS and FTP Download tabs are organized by firmware version, major release, and patch release. The firmware images in the folders follow a specific naming convention and each firmware image is specific to the device model. For example, the FMG_300D-v500-build0310-FORTINET.out image found in the */FortiManager/v5.00.5.0/5.0.6/* file folder is specific to the FortiManager 300D device model.

FortiManager VM firmware

Fortinet provides FortiManager VM firmware images for Amazon AWS, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

Amazon Web Services

- The 64-bit Amazon Machine Image (AMI) is available on the AWS marketplace.

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains the QCOW2 file for the Open Source Xen Server.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains QCOW2 that can be used by qemu.

Microsoft Azure

The files for Microsoft Azure have AZURE in the filenames, for example `FMG_VM64_AZURE-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Azure.

Microsoft Hyper-V Server

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.

VMware ESX/ESXi

- `.out`: Download the 64-bit firmware image to upgrade your existing VM installation.
- `.ovf.zip`: Download the 64-bit package for a new VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

For more information see the FortiManager product data sheet available on the Fortinet web site, http://www.-fortinet.com/products/fortimanager/virtualappliances.html. VM installation guides are available in the Fortinet Document Library

SNMP MIB download

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main v5.00 file folder.

Build numbers

Firmware images are generally documented as build numbers. New models may be released on a branch based off of the regular firmware release. As such, the build number found in the *System Settings* > *General* > *Dashboard, System Information* widget and the output from the `get system status` CLI command displays this four-digit build number as the build number.

To confirm that you are running the proper build, the output from the `get system status` CLI command has a `Branch point:` field that displays the regular build number.

Firmware upgrade and support information

Please also refer to the applicable releases notes for more details before upgrading your device.

Upgrade and support information

Firmware Version	Build Number	Upgrade From	FortiOS Version Support
5.6.0	1557	5.4.0-5.4.3	5.6.0 5.4.1-5.4.5 5.2.0-5.2.11
Note: FortiManager 5.6.0 does not support ADOM version 5.0. FortiManager 5.6.0 supports only the following ADOM versions: 5.2, 5.4, and 5.6.			
Supported models: FMG-200D, FMG-300D, FMG-300E, FMG-400E, FMG-1000D, FMG-2000E, FMG-3000C, FMG-3000F, FMG-3900E, FMG-4000D, and FMG-4000E; FMG-VM64, FMG-VM64-AWS, FMG-VM64-Azure, FMG-VM64-HV, FMG-VM64-KVM, and FMG-VM64-XEN (for both Citrix and Open Source Xen).			
5.4.2	1151	5.4.0-5.4.1 5.2.0–5.2.9	5.4.1-5.4.3 5.2.0-5.2.10 5.0.4-5.0.14
Note: With the enhancement in password encryption, FortiManager 5.4.2 does not support FortiOS 5.4.0. You need to upgrade FortiGate to 5.4.2. ADOM versions 5.0 and 5.2 are not affected.			
Supported models: FMG-200D, FMG-300D, FMG-300E, FMG-400E, FMG-1000D, FMG-2000E, FMG-3000C, FMG-3000F, FMG-3900E, FMG-4000D, and FMG-4000E; FMG-VM64, FMG-VM64-AWS, FMG-VM64-Azure, FMG-VM64-HV, FMG-VM64-KVM, and FMG-VM64-XEN (for both Citrix and Open Source Xen).			
5.4.1	1082	5.4.0 5.2.0–5.2.7	5.4.1-5.4.2 5.2.0-5.2.10 5.0.4-5.0.12
Note: With the enhancement in password encryption, FortiManager 5.4.1 does not support FortiOS 5.4.0. You need to upgrade FortiGate to 5.4.1. ADOM versions 5.0 and 5.2 are not affected.			
Supported models: FMG-200D, FMG-300D, FMG-300E, FMG-400E, FMG-1000D, FMG- 2000E, FMG-3000C, FMG-3000F, FMG-3900E, FMG-4000D, and FMG-4000E; FMG-VM64, FMG-VM64-AWS, FMG-VM64-Azure, FMG-VM64-HV, FMG-VM64-KVM, and FMG-VM64-XEN (for both Citrix and Open Source Xen).			
5.4.0	1019	5.2.0–5.2.4	5.4.0 5.2.0–5.2.7 5.0.4–5.0.12
Supported models: FMG-200D, FMG-300D, FMG-300E, FMG-1000D, FMG-3000C, FMG-3900E, FMG-4000D, and FMG-4000E; FMG-VM32, FMG-VM64, FMG-VM64-AWS, FMG-VM64-HV, FMG-VM64-KVM, and FMG-VM64-XEN (for both Citrix and Open Source Xen).			
5.2.9	0780	5.2.0-5.2.7 5.0.6–5.0.10	5.2.0–5.2.10 5.0.4–5.0.14 4.3.2–4.3.18

Firmware Version	Build Number	Upgrade From	FortiOS Version Support
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-300E, FMG-400C, FMG-400E, FMG-1000C, FMG-1000D, FMG-2000E, FMG-3000C, FMG-3000F, FMG-3900E, FMG-4000D, and FMG-4000E; FMG-VM64, FMG64-AWS, FMG-VM64-HV, FMGVM64-KVM, and FMG-VM64-XEN (for both Citrix and Open Source Xen).			
5.2.7	0757	5.2.0-5.2.6 5.0.6–5.0.10	5.2.0–5.2.7 5.0.4–5.0.13 4.3.2–4.3.18
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-300E, FMG-400C, FMG-400E, FMG-1000C, FMG-1000D, FMG-3000C, FMG-3900E, FMG-4000D, and FMG-4000E; FMG-VM64, FMG-VM64-XEN (for both Citrix and Open Source Xen), FMGVM64-KVM. FMG64-AWS, and FMG-VM64-HV.			
5.2.6	0753	5.2.0-5.2.4 5.0.6–5.0.10	5.2.0–5.2.7 5.0.4–5.0.13 4.3.2–4.3.18
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-300E, FMG-400C, FMG-400E, FMG-1000C, FMG-1000D, FMG-3000C, FMG-3900E, FMG-4000D, and FMG-4000E; FMG-VM32, FMG-VM64, FMG-VM64-XEN (for both Citrix and Open Source Xen), FMGVM64-KVM. FMG64-AWS, and FMG-VM64-HV.			
5.2.4	0738	5.2.0–5.2.3 5.0.6–5.0.10	5.2.0–5.2.4 5.0.4–5.0.10 4.3.2–4.3.8
Supported models:FMG-100C, FMG-200D, FMG-300D, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000C, FMG-3900E, FMG-4000D, and FMG-4000E; FMG-VM32, FMG-VM64, FMG-VM64-XEN (for both Citrix and Open Source Xen), FMGVM64-KVM. FMG-VM64-AWS, and FMG-VM64-HV.			
5.2.3	0724	5.2.0–5.2.2 5.0.6–5.0.10	5.2.0–5.2.4 5.0.4–5.0.10 4.3.2–4.3.8
Supported models:FMG-100C, FMG-200D, FMG-300D, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000C, FMG-3900E, FMG-4000D, and FMG-4000E; FMG-VM32, FMG-VM64, FMG-VM64-XEN (for both Citrix and Open Source Xen), FMGVM64-KVM, FMG-VM64-AWS, and FMG-VM64-HV.			
5.2.2	0706	5.2.0–5.2.2 5.0.6–5.0.10	5.2.0–5.2.3 5.0.4–5.0.10 4.3.2–4.3.8
Supported models: FMG-100C, FMG-200D, FMG-200E, FMG-300D, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000C, FMG-3900E, FMG-4000D,and FMG-4000E; FMG-VM32, FMG-VM64, FMG-VM64-XEN (for both Citrix and Open Source Xen), FMGVM64-KVM. FMG-VM64-AWS, and FMG-VM64-HV.			
5.2.1	0662	5.2.0 5.0.8, 5.0.9	5.2.0–5.2.2 5.0.4–5.0.10 4.3.2–4.3.8

Firmware Version	Build Number	Upgrade From	FortiOS Version Support
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000C, FMG-3900E, FMG-4000D, and FMG-4000E; FMG-VM32, FMG-VM64, and FMG-VM64-HV.			
5.2.0	0618	5.0.6– 5.0.9	5.2.0, 5.2.1 5.0.4–5.0.9 4.3.2–4.3.8
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000C, FMG-4000D, FMG-4000E, FMG-VM32, FMG-VM64, and FMG-VM64-HV.			

Upgrading to FortiManager 5.6.0

You can upgrade FortiManager 5.4.0 or later directly to FortiManager 5.6.0.

If you are upgrading from versions earlier than 5.4.x, you should upgrade to FortiManager 5.4.x first. (We recommend that you upgrade to the latest version of FortiManager 5.4.) See also Firmware upgrade and support information on page 6.

FortiManager 5.6 supports the following ADOM versions: 5.2, 5.4, and 5.6. FortiManager 5.6 does not support the 5.0 version of ADOMs. If your FortiManager currently includes version 5.0 ADOMs, you must upgrade the 5.0 ADOMs to 5.2 or later before you upgrade the firmware of FortiManager to 5.6.0.

Upgrading 5.0 ADOMs to 5.2 ADOMs

Before you upgrade the firmware of FortiManager to 5.6.0, you must upgrade all 5.0 ADOMs to 5.2 or later ADOMs because FortiManager does not support 5.0 ADOMs.

To upgrade ADOM version 5.0 to 5.2:

1. In the 5.0 ADOM, upgrade one of the FortiGate units to FortiOS 5.2, and then resynchronize the device.
   All of the ADOM objects, including Policy Packages, remain as 5.0 objects.
2. Upgrade the rest of the FortiGate units in the 5.0 ADOM to FortiOS 5.2.
3. Upgrade the ADOM to version 5.2.
   a. Ensure that you are logged into FortiManager as a super user administrator.
   b. Go to *System Settings* > *All ADOMs*.
   c. Right-click an ADOM and select *Upgrade*.
   d. Select *OK* in the confirmation dialog box to upgrade the device.
      If all of the devices in the ADOM are not already upgraded, the upgrade will be aborted, and an error message is displayed. Upgrade the remaining devices in the ADOM, and then upgrade the ADOM again.

All of the database objects will be converted to 5.2 format, and the GUI content for the ADOM will change to reflect 5.2 features and behavior.

Upgrading FortiManager Firmware

The following table lists the firmware upgrade steps.

Upgrade steps

Step 1	Prepare your device for upgrade.

Step 2	Back up your system configuration.
Step 3	Transfer the firmware image to your device.
Step 4	Log into the GUI to verify the upgrade was successful.

Step 1: Prepare your device for upgrade

1. Ensure that you upgraded all 5.0 ADOMs to 5.2 or later ADOMs. See Upgrading 5.0 ADOMs to 5.2 ADOMs on page 10.
2. Install any pending configurations.
3. Make sure all managed devices are running the supported firmware versions.
4. Log into the Fortinet Customer Service & Support portal at https://support.fortinet.com.
5. Click *Download* on the toolbar and select *Firmware Images* from the drop-down menu.
6. Select *FortiManager* from the *Select Product* drop-down list, and navigate to the directory for version 5.6.0.
7. Select the image for your FortiManager model and download it to your management computer. You can click *HTTPS* to download the image via a HTTPS connection.
8. To verify the integrity of the download, click the *Checksum* link for the image that you selected. The checksum code and image file name are displayed in the Get Checksum Code dialog box that opens.

Step 2: Back up your system configuration

1. Go to *System Settings* > *Dashboard*.
2. Select *Backup* in the *System Information* widget. The *Backup* dialog box opens.
3. Select the check box to encrypt the backup file and enter a password.
4. Select *OK* and save the backup file on your local computer.

When selecting to encrypt the backup configuration file, the same password used to encrypt the file will be required to restore this backup file to the device.

Optionally, you can back up the configuration file to a FTP, SFTP, or SCP server using the following CLI command:

```
execute backup all-settings {ftp | sftp} <ip>
    <path/filename save to the server> <username on
    server> < password> <crptpasswd>

execute backup all-settings scp <ip> <path/filename save
    to the server> <SSH certificate> <crptpasswd>
```

For more information, see the *FortiManager CLI Reference*.

Step 3: Transfer the firmware image to your device

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, in the *Firmware Version* field, Click *Upgrade Firmware*. The *Firmware Upload* dialog box opens.

3. Select *Browse* to locate the firmware package (`.out` file) that you downloaded from the Customer Service & Support portal and select *Open*.
4. Select *OK*. Your device will upload the firmware image and you will receive a confirmation message noting that the upgrade was successful.

Optionally, you can upgrade firmware stored on an FTP or TFTP server using the following CLI command:

```
execute restore image {ftp | tftp} <file path to server>
    <IP of server> <username on server> <password>
```

For more information, see the *FortiManager CLI Reference*.

Step 4: Log into the GUI to verify the upgrade was successful

1. Refresh the browser and log back into the device.
2. Launch the *Device Manager* module and make sure that all formerly added devices are still listed.
3. Select each ADOM and make sure that managed devices reflect the appropriate connectivity state. Optionally, go to *System Settings* > *All ADOM*s.
4. Launch other functional modules and make sure they work properly.

Upgrading the firmware for an operating cluster

You can upgrade the firmware of an operating cluster through the GUI or CLI of the primary unit.

Similar to upgrading the firmware of a standalone unit, normal operations are temporarily interrupted during the cluster firmware upgrade. Therefore, you should upgrade the firmware during a maintenance window.

To upgrade a HA cluster:

1. Log into the GUI of the primary unit using the `admin` administrator account.
2. Upgrade the primary unit firmware. The upgrade is automatically synchronized between the primary device and backup devices.

Administrators may not be able to connect to the GUI until the upgrade synchronization process is completed. During the upgrade, SSH or telnet connections to the CLI may also be slow. You can still use the console to connect to the CLI of the primary device.

Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous firmware release via the GUI or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset {all-settings | all-except-ip}
execute format {disk | disk-ext4 | disk-ext3}
```